$$\frac{\mathbf{A}\,\mathbf{A}'}{a^2}+\frac{\mathbf{B}\,\mathbf{B}'}{b^2}+\frac{\mathbf{C}\,\mathbf{C}'}{c^2}$$

and the radius vector $\circ\mathbf{a}+\circ\mathbf{b}+\circ\mathbf{c}$ which gives $\dfrac{\circ\mathbf{A}}{a}+\dfrac{\circ\mathbf{B}}{b}+\dfrac{\circ\mathbf{C}}{c}$. Having the normal it is easy to construct the equation of the tangent plane.

It may be remarked that if the preceding equations were written in one of the usual notations, as, for instance, that used by Gibbs, they would become very complicated, though the concepts represented, as we have seen are simple enough.

5. Neither the usual vector equations, those just given, nor the cartesian equations, possess exclusive merits over the others. Each in turn can be superior to the others for certain purposes. It is easier to construct the curves and surfaces from the equations just given than from the cartesian equations since one can use the trigonometric tables. The equations for the *plane* curves do not differ except in compactness and convenience of notation from the vector equations commonly given. But those for space of three dimensions are new forms. Writers on vector analysis use the ϕ function for quadrics, which introduces very compact expressions, but ones essentially scalar. The use of the above equations makes the treatment of solid space analogous to that of plane and connects vector analysis much more closely to cartesian analysis.

NOTE ON THE TOTIENT OF A NUMBER.

By G. A. MILLER.

Like the preceding paper, "On the Totitives of Different Orders," MONTHLY, Vol. XI, p. 129, this note aims to point out the advantages of employing the theory of groups in the proofs of some of the elementary theorems of number theory.

The number of natural numbers which do not exceed the positive integer m and are prime to m is denoted by $\phi(m)$ according to Gauss.* This function of m is known by various names. English, French, and German writers respectively employ the following names: totient of m, indicator of m, Euler's ϕ-function of m. If 1, d_1, d_2, ..., d_λ, m are all the divisors of m it is well known that

$$\phi(1)+\phi(d_1)+\phi(d_2)+\dots\dots\dots+\phi(d_\lambda)+\phi(m)=m.$$

The main object of this note is to show the connection between this formula and the theory of cyclic groups in a very elementary manner. Several closely related questions in number theory are also treated from the standpoint of group theory.

*Gauss, *Disquisitiones Arithmeticae*, Art. 88.

If d is any divisor of m then there is one and only one subgroup of order d in the cyclic group (G) of order m. This subgroup is cyclic. Hence there are just $\phi(d)$ operators of order d in G. Moreover, the order of every operator of G is a divisor of m. The given formula therefore says nothing more than that *the sum of the numbers of the operators of the different possible orders is equal to the order of G*. That is, this formula exhibits a very elementary property of cyclic groups and requires no further proof if the given properties of cyclic groups are assumed to be known. We proceed to give a simple proof of these properties.

Since d is a divisor of m any generator (s) of G must contain a cyclic subgroup of order d. It cannot contain more than one such subgroup because the 1st, 2d, ..., mth powers of s contain only d operators whose orders divide d,* and these powers give all the operators of G. These statements prove that G contains one and only one subgroup of order d and that this subgroup is cyclic.

The given formula may clearly be regarded as a special case of the following evident theorem. *If g is the order of any finite group and if* $1, d_1, d_2, \ldots, d_\gamma$ *are the orders of all of its cyclic subgroups, then*

$$\phi(1)+\phi(d_1)+\phi(d_2)+\ldots\ldots+\phi(d_\gamma)=g.$$

Since every non-cyclic group contains more than one cyclic subgroup of the same order, it follows that the given $\gamma+1$ divisors of g cannot all be different unless the group is cyclic. In this special case we arrive at the preceding formula, as has been proved above.

The given properties of the cyclic group may be employed to obtain very elementary proofs of the formulas $\phi(mn)=\phi(m)\phi(n)$ whenever m and n are prime to each other, and

$$\phi(m)=m(1-\frac{1}{p_1})(-\frac{1}{p_2})\ldots\ldots(1-\frac{1}{p_\rho})$$

where $p_1, p_2, \ldots\ldots, p_\rho$ are all prime factors of m.

The former of these two formulas gives the number of operators of highest order in the cyclic group of order mn, m and n being relatively prime. This cyclic group contains just one cyclic subgroup of each of the orders m and n, and it is the direct product of these two cyclic subgroups since they have only the identity in common. To obtain an operator of order mn it is necessary to multiply an operator of order m from the first subgroup into an operator of order n from the second subgroup, and all such products are of order mn. Hence the number of operators of highest order in the entire group is the product of the numbers of the operators of highest order from the two subgroups. In other words, $\phi(mn)=\phi(m)\phi(n)$.

All the subgroups of a cyclic group of order p^α, p being a prime, are con-

*From $(s^x)^d=1$ it follows that $xd=km$, or $x=km/d$. Hence x has one of the values m/d, $2m/d$, ... dm/d mod$m$.

tained in its subgroup of order $p^{\alpha-1}$. That is, $\phi(p^{\alpha})=p^{\alpha}-p^{\alpha-1}=p^{\alpha}(1-1/p)$. If $m=p_1^{\alpha_1}p_2^{\alpha_2}\ldots\ldots p_\rho^{\alpha_\rho}$, it follows from this and the preceding formula that

$$\phi(m)=\phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\ldots\ldots\phi(p_\rho^{\alpha_\rho})$$

$$=p_1^{\alpha_1}p_2^{\alpha_2}\ldots\ldots p_\rho^{\alpha_\rho}(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots\ldots(1-\frac{1}{p_\rho})$$

$$=m(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots\ldots(1-\frac{1}{p_\rho}).$$

It may be observed that the formula $\phi(p^{\alpha})=p^{\alpha-1}(p-1)$ may be regarded as a special case of the formula $\phi(m^r)=m^{r-1}\phi(m)$, since $\phi(p)$ is evidently equal to $p-1$.

AN APPLICATION OF STIRLING'S INTERPOLATION FORMULA

By FRANK ELMORE ROSS.

Let write the values of $\sin x$ for $x=0$, π, etc., and form the series of differences, as in the ordinary process of interpolation. The result is as follows, Δ_n denoting the nth difference:

x	$\sin x$	Δ_1	Δ_2	Δ_3	Δ_4	Δ_5	....
0	0						
		+1					
$\frac{1}{2}\pi$	+1		−2				
		−1		+2			
π	0		0		0		
		−1		+2		−4	
$3\pi/2$	−1		+2		−4		....
		+1		−2		+4	
0	0		0		0		....
		+1		−2		+4	
$\frac{1}{2}\pi$	+1		−2		+4		
		−1		+2			
π	0		0				
		−1					
$3\pi/2$	−1						

This scheme extends infinitely in both directions, the difference Δ_n forming a divergent series. It is found however that a convergent series for the